OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

August 11, 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Interim Guidance for the Department of Defense (DoD) Public Key Infrastructure (PKI)

As the U.S. military and intelligence community redefine the way in which information will be accessed and used in the 21st century, the collective needs of the warfighter, theatre commanders, support elements, and leaders at Defense and national levels must be addressed in the context of *Information Superiority*. The DoD PKI will provide the critical underpinning of our Information Assurance capabilities across the Department, and thus our ability to achieve Information Superiority. Our ability to make consistent *risk management* decisions, in full consideration of the highly interconnected, interdependent, shared risk environment in which we conduct our daily operations, is inextricably linked to the services provided by the DoD PKI. Accordingly, I believe we must take an aggressive approach in establishing a PKI that meets our requirements for all information assurance services. The goal of this DoD-wide infrastructure is to provide general purpose PKI services, e.g., issue certificates supporting digital signature and encryption, provide directory services, enable the revocation of certificates, etc., to a broad range of applications, at the levels of assurance consistent with operational mission imperatives.

The DoD PKI must avoid the significant duplication of effort and costs that are incurred by unique and non-interoperable systems, enable the outsourcing of appropriate PKI activities and functions to achieve economies of scale, and must satisfy major program and operational requirements. Further, the DoD PKI must support the recovery of encryption keys for information as it traverses the network and while at rest. Finally, the PKI must comply with and support applicable DoD policies.

Within the next thirty (30) days, the Information Assurance Directorate will staff three critical documents:

a. DoD X.509 Certificate Policy
b. DoD Certification Practice Statement
c. DoD Public Key Infrastructure (PKI) Roadmap

These documents will contribute to establishing the enterprise-wide end-state for the DoD PKI, provide the foundation for our PKI *strategy*, and ensure that, Department-wide, we are consistent in identifying PKI assurance levels commensurate with mission objectives. They will establish the timeline for availability of PKI capabilities and ensure that we are able to outsource, as appropriate, functions supporting low value and non-mission critical transactions at the earliest possible time. It is essential that you give these documents the widest possible dissemination. Your comments will ensure that the DoD PKI strategy derived from this baseline meets, to the maximum extent possible, your operational mission requirements.

Until we have fully coordinated these documents and developed a Department-wide PKI strategy, no new certificate infrastructures shall be established without prior written approval of the DoD Chief Information Officer (CIO). Ongoing pilots may be continued but costs should be minimized and risk management decisions shall be thoroughly reviewed by the Designated Approving Authority (DAA) of the pilot to ensure that inappropriate risk to the interconnected networks has not been accepted.

Additional applications, beyond ongoing pilots, wishing to use the current medium assurance pilot infrastructure must, prior to implementation, conduct a risk assessment describing the services required from the infrastructure as well as the sensitivity of the information being protected. DISA and NSA will provide guidance concerning the information to be included in the risk assessment, and the DoD PKI Senior Steering Committee will grant approval for use of the medium assurance infrastructure. In addition, these pilots will be required to report on their "lessons learned" from the pilot activities in support of enterprise-wide PKI decisions and plans. Guidance for the data tc be reported by the pilot will be provided in the Roadmap document, mentioned above.

Our goal for establishing the *DoD PKI Strategy* and formal release of the referenced documents is January 15, 1999. My point of contact for this action is Richard C. Schaeffer, Jr., OASD(C3I), Director, Information Assurance, telephone: (703) 695-8705.

Arthur L. Money
Senior Civilian Official